Net Load Redistribution Attacks on Nodal Voltage Magnitude Estimation in AC Distribution Networks

Hang Zhang, Bo Liu, and Hongyu Wu
The Department of Electrical & Computer Engineering
Kansas State University, Manhattan, United States, 66506

***Abstract*—A high penetration level of smart devices and communication networks increases the threat of cyber-attacks in the distribution system. In this paper, we model a hidden, coordinated, net load redistribution attack (NLRA) in an AC distribution system. Based on local information of an attack region, the attacker's goal is to create violations in nodal voltage magnitude estimation. Acting as a system operator equipped with global AC state estimation and bad data detection, we validate the stealthiness of the hidden NLRA in multiple attack cases. Simulation results on a modified PG&E 69-node distribution system show the validity of the proposed NLRA. The influence of NLRA on the distribution system is assessed and the impact of attack regions, attack timing, and system observability is also revealed.**

***Index Terms*—false data injection attacks, load redistribution attacks, voltage violation, bad data detection.**

I. Introduction

Electric power systems are under rapid and revolutionary development towards smart, autonomous, and communicational technologies. A number of smart meters and phasor measurement units (PMUs) are increasingly utilized to monitor power system states. These sensors are susceptible to a growing risk of cyber-attacks due to the vulnerability of the communication networks [1]. For example, the 2015 Ukraine blackout is a consequence of an adversary, stealthily compromising measurements from electricity grid sensors in a coordinated fashion [2].

Cyber data attacks are viewed as "the worst interacting bad data injected by an adversary" [3]. In [4], Liu *et al.* analyzed several existing security accidents and introduced the taxonomy of the attacks according to their spatial-temporal characteristics. An attacker with the capability of configuration information can manipulate the measurement data at the smart meters as they are usually physically exposed [5]. Such attacks are defined as false data injection (FDI) [3], [6], [7]. FDI attacks result in incorrect state estimation and further undermine the economic and secure operation of power systems. In previous research, it is assumed attackers have the entire power network information. In reality, this is an impractical assumption due to the security and complexity of today's power grid. Therefore, FDI attacks with incomplete information [8]–[12] are drawing more research attention. In [9], Liu *et al.* demonstrate an attacker could construct an undetectable FDI attack in an AC transmission system with incomplete network information by maintaining the same phase angle increment at the boundary nodes of the attack region. According to the characteristics of transmission systems (i.e., high X/R ratio, meshed network), Liu *et al.* proposed a method to optimally estimate phase angle differences between boundary nodes [10]. Their results showed the construction of an FDI attack does not require knowledge of the entire power network. Yuan *et al*. developed a novel concept of load redistribution attacks (LRA) [13], which is a more realistic form of the FDI attack in the DC transmission system. To the best of our knowledge, the LRA has not been researched in AC distribution systems with distributed energy resources (DERs), wherein the malicious measurement may be disguised by the uncertain DERs' power injection. Existing research on the effect of LRA mainly concerns with economic consequences. However, little research has been conducted when attackers aim at creating system state violations.

Unlike a transmission system, the distribution system is characterized by a radial network typology and a low X/R ratio. Therefore, the method proposed in [10] does not apply to the distribution system as significant approximation errors occur in the estimation of voltage angle differences in the distribution system. Furthermore, there has been little effort to model a stealthy FDI attack with a tangible attack goal in the distribution system. Without such a goal, it is impossible for a defender to analyze the real consequence of an FDI attack.

In this paper, we propose a novel net load redistribution attack (NLRA) aiming at falsifying nodal voltage magnitude estimation in the AC distribution system. Specifically, the attackers intend to create illusory voltage violations such as under-voltage violations to the system operator. Unlike previous research [13], [14] with a strong common assumption that the attacker must have complete knowledge about the entire power grid network, we model NLRA as an attacker's AC optimal power flow (OPF) problem that only requires local distribution network information. The NLRA model is solved by using an interior-point algorithm and simulations are conducted on a modified PG&E 69-node distribution system. It is worth mentioning that the intention of this paper is not to educate the attackers on how to perform FDI attacks, but to provide power grid operators with a better understanding of attack consequences, which in turn can assist in devising effective defense approaches.

The rest of this paper is organized as follows. The background on hidden FDI attacks against the AC state estimation is given in Section II. The construction of the NLRA attack using local measurements in the targeted region is presented in Section III. Case studies on the modified 69-node distribution system are discussed in Section IV. This paper is concluded in Section V.

II. Hidden FDI Attacks against AC State Estimation

Bad Data Detection (BDD) in AC state estimation is based on a residual analysis of $\mathbf{r} = \mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})$, where $\mathbf{r}$ is the residual, $\hat{\mathbf{x}}$ is the estimated system states, $\mathbf{z}$ is the measurements, and $\mathbf{h}(\cdot)$ is a nonlinear function between the system states and the measurements. The residual can be attributed to noise and inaccuracy of the measurements as well as injected false data. The defender, usually a distribution system operator (DSO), runs the BDD tests by comparing the residual with a pre-defined threshold τ calculated at a certain confidence interval.

$$\|\mathbf{r}\|_2 = \|\mathbf{z} - \mathbf{h}(\hat{\mathbf{x}})\|_2 < \tau \tag{1}$$

When there is at least one faulty measurement, the l_2-norm of residual exceeds the threshold.

To launch a stealthy AC FDI attack with incomplete network information, two conditions need to be satisfied. First, the attack vector itself should bypass the BDD tests. Liu *et al*. [7] proved that if an attacker injects false data that are consistent with the physical characteristics of power systems into the measurements, the attack vector can bypass the BDD. Second, the injected attack vector should not cause any state or measurement changes outside of the attack region since the attacker does not have access to the non-attack region. Liu *et al.* [9] demonstrated that if an attack vector ensures that all boundary nodes between the attack and non-attack regions have the same incremental phase angle, the additional power flow due to the injected false power will not flow out of the attack region. Therefore, the power system states and measurements in the non-attack region would remain unchanged.

III. Proposed Attack Model

Cyber-attacks on a certain type of power system measurements can easily expose themselves. For example, a cyber-attack on the measurements of a utility-scale wind or solar farm can be straightforwardly detected through direct communication between the system control center and the generating resource control room [14]. A nodal net load, calculated as the total load minus the total local generation, is measured at a specific node in the power system. Nodal net load measurements would become highly uncertain with a greater amount of behind-the-meter DERs in the distribution system, giving rise to cyber-attacks as the attacker can disguise an attack vector as uncertainties.

We investigate a stealthy FDI attack model, termed as NLRA, in which measurements on the net power injection at a load node and related line power flow measurements can be compromised. With some mild assumptions on the attackers' capability, attackers can precisely control the errors injected into these measurements (attack vector) in a coordinated manner to mislead the estimation of nodal voltage magnitudes in the attack region. The attackers must also maintain the sum of all net power injection measurements in the attack region unchanged to make the attack stealthy.

A. Attacker's Capabilities

To meet the two conditions discussed in Section II and launch a stealthy NLRA attack, an attacker must have the following capabilities:

1) Knowledge of line impedance in the attack region. In reality, line impedance may not be directly accessible to the attackers. They need to launch data exfiltration attacks to obtain the line impedance. Several methodologies [15]–[18] have been proposed to estimate the line impedance;

2) Read & write access to power injection and line flow measurements in the attack region. The attacker can eavesdrop on those measurements and perform man-in-the-middle attacks; and

3) Read access to the voltage magnitude and angles at boundary nodes as well as read access to the tie-line power flow between the attack and non-attack regions.

Table I. Attacker's capabilities for NLRA

Measurements	Capabilities
Line impedance	Attack region (Knowledge)
Power injection	Attack region (Read & Write)
Line power flow	Attack region (Read & Write) Tie lines (Read-only)
Voltage magnitude	Boundary nodes (Read-only)
Voltage angle	Boundary nodes (Read-only)

The attacker's capabilities required to launch a stealthy NLRA are summarized in Table I. Note that the attacker's cost (e.g., resources invested) to launch a successful NLRA is highly related to the scale of an attack region. For an attacker, attacking a large region requires a higher cost than a small region, but may result in more severe consequences in the distribution system.

B. Attack Objectives

The attacker's goal is to mislead the DSO to observe under-voltage issues in AC state estimation by injecting attack vector into the measurements. Let A, B, T represent the set of nodes in the attack region, boundary nodes, and tie lines, respectively. The objective of the NLRA attack is formulated below.

$$\min \sum_{a \in A} c_a V_a \tag{2}$$

Here, subscript a denotes the targeted nodes in the attack region A; V_a represents the intended voltage magnitude measurements of node a; c_a is a non-negative weight coefficient assigned to node a representing the attack emphasis, the summation of which equates to 1. To achieve the most desirable under-voltage violation, an attacker can assign a large weight to the most critical node, and a zero weight for nodes of no interest.

C. Stealthy Conditions

To make NLRA stealthy, an attacker needs to ensure measurements of the tie line's power flow S_T, the voltage

magnitude on the boundary nodes V_B, and the voltage phase difference between the boundary nodes $\Delta\theta_B$ remain unchanged after the attack as defined in (3).

$$\begin{bmatrix} S_T \\ V_B \\ \Delta\theta_B \end{bmatrix} = \begin{bmatrix} S_T' \\ V_B' \\ \Delta\theta_B' \end{bmatrix} \tag{3}$$

Here, superscript $(\bullet)'$ denotes the measurements before an attack. Constraints (4) and (5), showing the essence of an NLRA, indicate the sum of all net load changes should be equal to zero, and the net load's change at each node is within a reasonable range, respectively.

$$\sum_{a\in A} \Delta D_a = 0 \tag{4}$$

$$-\delta S_a^{l\prime\prime} \le \Delta D_a \le \delta S_a^{l\prime\prime} \tag{5}$$

In (4), ΔD_a is the attack magnitude, i.e., net load change, at each node in the attack region. In (5), δ is a percentage of allowable change on the original load (apparent power) measurement $S_a^{l\prime}$. Constraint (5) is imposed because the DSO can check the sensor measurements when an under-voltage condition occurs. In this case, unrealistic injected data can be easily exposed.

With local information of the attack region and boundary information between the attack and non-attack regions, NLRA is modeled as a modified ACOPF problem, in which the prevailing ACOPF constraints (6) – (10) hold for the proposed NLRA.

$$S^l = P^l + iQ^l \tag{6}$$

$$g_P(\theta, V, P^l) = 0 \tag{7}$$

$$g_Q(\theta, V, Q^l) = 0 \tag{8}$$

$$h_f(\theta, V) \le 0 \tag{9}$$

$$h_t(\theta, V) \le 0 \tag{10}$$

Here, voltage angle θ, voltage magnitude V, real and reactive power load P^l and Q^l are decision variables. In (7), g_P is the nonlinear equality constraints of nodal real power balance. In (8), g_Q represents the nonlinear equality constraints of nodal reactive power balance. h_f in (9) and h_t in (10) are nonlinear inequality constraints of power flow limits at the "from node" and "to node", respectively. Attack vectors generated by the proposed NLRA model obey Kirchhoff's current & voltage laws, implying they follow the inherent characteristics of the distribution system.

D. Attack Simulation

The flow chart of an NLRA in the distribution system is shown in Fig. 1. The attacker has the capability of eavesdropping on compromised sensors in the attack region. The attacker can generate an attack vector by running the NLRA model formulated in (2)-(10) based on the eavesdropped measurements. Further, the attacker can inject the calculated attack vector back into the corresponding communication links through man-in-the-middle attacks.

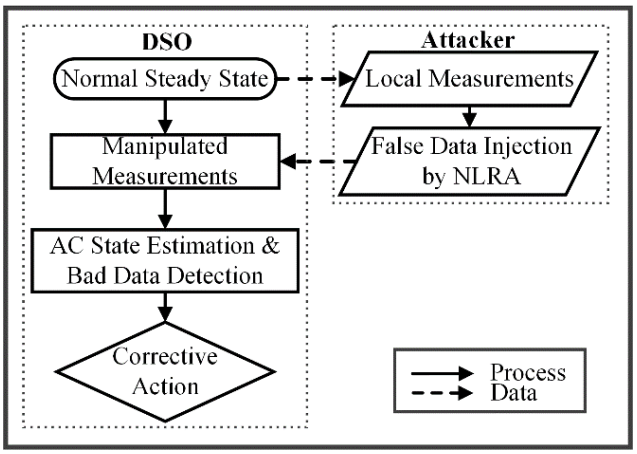


Fig. 1. The flowchart of NLRA

In this study, we assume that DSO is equipped with an AC state estimator and BDD. The AC state estimator utilizes compromised measurements combined with the measurements in the non-attack region to check the existence of a cyber-attack. If the attack bypasses the BDD test, the system will respond to the estimated system states with corrective actions. In this paper, we focus on demonstrating the impact of the NLRA attacks in the distribution system. Corrective actions, and most importantly, defense approaches for the DSO in response to NLRA are out of the scope of this paper.

IV. Case Study

In this section, the proposed NLRA model is simulated on a modified PG&E 69-node radial distribution system. The DSO, equipped with the AC state estimator and BDD, has full access to all sensor measurements and global information of the entire distribution system. We simulate NLRA on this system and assess its attack consequences while accounting for the impact of attack regions, attack timing, and system observability. The NLRA, AC state estimation, and BDD are all performed in MATPOWER [19].

A. Test Distribution System

The one-line diagram of the modified 69-node system is shown in Fig. 2. We modify the original PG&E 69-node radial distribution system by adding aggregated behind-the-meter DERs at certain nodes (in Fig. 2). We initially assume the system is fully observable and reduce its observability whereby the impact of the NLRA is studied. There are four PMUs installed at Nodes 13, 26, 53, and 63. In this case, there are 483 sensors in the system, including 211 nodal measurements (i.e., real and reactive power injections, voltage magnitude and phase angles at boundary nodes) and 272 line measurement (i.e., real and reactive power flow on both the "from node" and the "to node"). We simulate NLRA in two regions (i.e., main feeder and lateral) and three time periods (i.e., valley, shoulder, and peak hours). The range of allowable voltage magnitudes is between 0.95 p.u. and 1.05 p.u. in this system.

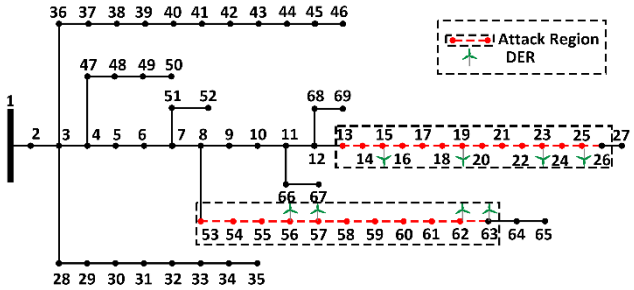


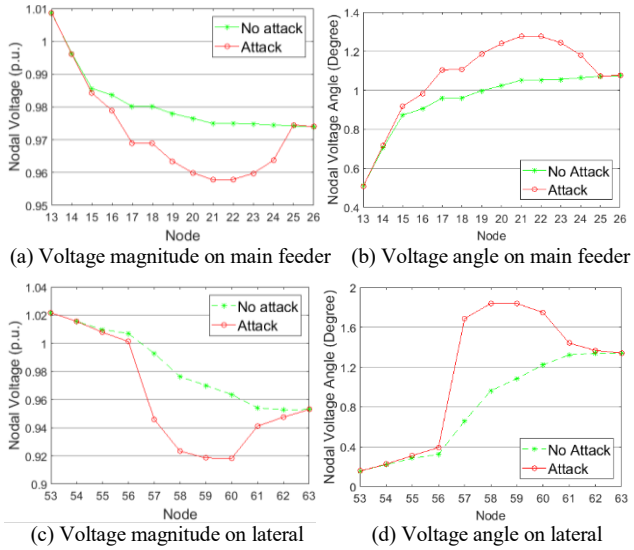
Fig.2. The modified PG&E 69-node system

B. *Impact of Attack Regions*

In this subsection, we compare the system impact of the attack at two regions, i.e., one on the main feeder (Nodes 13 to 26) and the other on the lateral (Nodes 53 to 63). To demonstrate the flexibility of attacking different numbers of nodes, we choose Nodes 22 to 25 on the main feeder and Node 59 on the lateral as targets, that is, the weight coefficients on these nodes are non-zero. While attackers may pick their target nodes of interest, here we randomly select the target nodes in the middle of the attack region. Such a selection allows the voltage magnitude profile to drop first and then rise to satisfy the boundary condition. This is a unique characteristic of the NLRA attacks in the radial distribution system. Fig. 3 shows nodal voltage magnitudes and angles at a peak hour before and after the attack. In order to make the NLRA stealthy in the attack region, the voltage magnitudes and the incremental phase angles on the boundary nodes remain the same after the attack. When the attack is on the main feeder, the largest voltage drop occurs at Node 21, which is 0.017 p.u. No voltage magnitude of any node drops below the secure range and the DSO observes no under-voltage issue. When the attack is on the lateral, the DSO perceives six voltage violations below the lower limit of 0.95 p.u. at Nodes 57 to 62. The largest voltage drop of 0.057 p.u. occurs at Node 58. The difference in attack consequences between the two attack regions is largely attributed to the difference in line impedance. Specifically, an attack region with higher line impedance would more likely experience larger voltage drops under an NLRA. Therefore, the optimal strategy for an attacker is to launch an NLRA on laterals, where the line impedance is higher than that of the main feeder.

C. *Impact of Attack Timing*

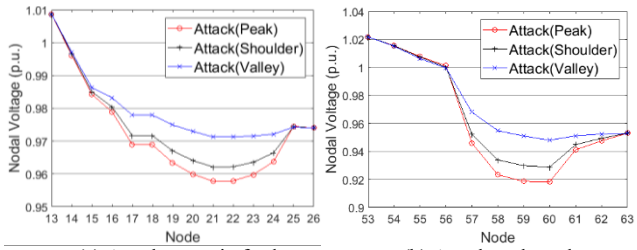
In this subsection, we investigate the impact of attack timing on the distribution system by implementing NLRA in different time periods. Figure 4 compares the profiles of voltage magnitudes after NLRA on the main feeder and the lateral at peak, shoulder, and valley hours. It is seen larger voltage drops occur during the peak hour in both attack regions. As shown in Fig. 4(b), on the lateral occur five and one nodal voltage violations at the shoulder and the valley hours, respectively. The most severe attack consequences occur on the lateral during the peak hour when the under-voltage condition occurs on six nodes, i.e., Nodes 57-62. This result can be explained by comparing the net load differences at those time periods. A higher load condition provides NLRA with more freedom to manipulate and redistribute the nodal net loads in the attack region.



(a) Voltage magnitude on main feeder (b) Voltage angle on main feeder

(c) Voltage magnitude on lateral (d) Voltage angle on lateral

Fig. 3. Attack consequences on a peak hour



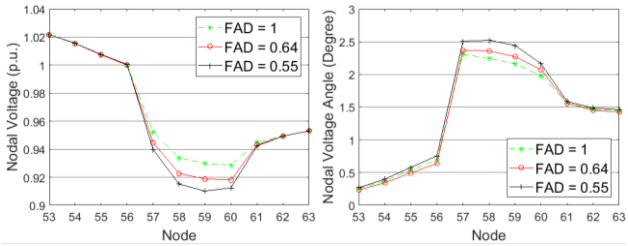
(a) Attack on main feeder (b) Attack on lateral

Fig. 4. Attack consequences in different time periods

D. *Impact of System Observability*

We analyze attack consequences with different levels of observability in the distribution system. Although the deployment of various recent technologies, such as advanced metering infrastructure, PMUs, intelligent electronic devices, and smart inverters of DERs, have improved the network observability, the distribution system is generally underdetermined with poor observability and easily becomes unobservable due to the communication failure and delay [20].

Here, we adopt a metric developed in our previous work [21], namely fraction of the available data (FAD), to reflect the distribution system observability. FAD is defined as the ratio of the number of measurements deployed over the total number of possible measurements in a region. Figure 5 compares the voltage magnitudes and angles at three different FADs in the lateral attack region. When FAD is set to 0.64 and 0.55, we randomly select four and five unmeasured nodes in the attack region, respectively. An unmeasured node indicates that no measurements, including its nodal power injection and associated branch flows, are available to the operator. Compared with the base case where the system is fully observable (FAD=1), the NLRA with a lower FAD can result in large attack impact and more voltage violations, translating to a more severe under-voltage issue. This is because fewer sensors deployed in the system leads to a more unobservable system, where the attacker would have more flexibility to launch a more coordinated NLRA.



(a) Voltage magnitude on lateral (b) Voltage angle on lateral

Fig. 5. Attack consequence with different FADs

E. Impact of the Size of an Attack Region

In this subsection, we study the impact of the size of an attack region on the stealthiness of the NLRA. We reduce the size of the attack region by randomly selecting 4 to 7 nodes out of the total 11 nodes (Nodes 53-63) on the lateral as the attack region. For each attack region, we simulate NLRA, the AC state estimation, and the BDD tests 1000 times. In order to show the stealthiness of the NLRA, we use an attack stealthiness probability (ASP) metric, which is defined as the probability of the attack vector bypassing the BDD test. Due to the meter measurement noise, the residual check for a normal system fails with a probability of 0.02 to 0.05, which gives the non-attack case an ASP between 0.95 to 0.98. Fig. 6 shows the ASP of the four attack sizes. It is seen ASP increases as the size of the attack region increases. This is because the larger the attack region is, the more noise-free measurements there will be. The noise-free measurements are the injected false data, which strictly obey Kirchhoff's current and voltage laws and thus reduce the residual in the AC state estimation.

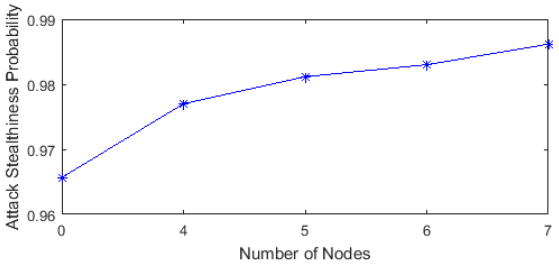


Fig. 6. ASP versus the number of nodes in the attack region

V. Conclusion and Future Work

Based on the concept of the LRA, this paper proposes a stealthy NLRA against the AC distribution system with behind-the-meter DERs using local network information. The proposed method is stealthy to BDD in the state estimator and can mislead DSO with illusory under-voltage issues. The numerical results show that the estimation residual after the NLRA is smaller than that before the attack, which can ensure the stealthiness of NLRA. The simulation results demonstrate that a larger attack area in NLRA further reduces the residual in BDD. The NLRA attacks aiming at the region with higher line impedance (e.g., laterals) and larger total net load (e.g., the peak load) lead to larger voltage drops in the attack region. Furthermore, lower system observability increases the adverse impact of NLRA on the distribution system. Our future work will focus on the development of a defense framework in which the proposed NLRA will be simulated. Attack sequences with a high level of DERs as well as other attack goals in the distribution system will be also be researched.

Acknowledgment

This material is based upon work supported in part by the U.S. National Science Foundation under Grant No. 1929147, and in part by the U.S. Department of Energy under Award No. DE-EE0008767.

References

[1] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *2010 First IEEE International Conference on Smart Grid Communications*, Gaithersburg, MD, USA, 2010, pp. 220–225.

[4] T. Liu *et al.*, "Integrated security threats and defense of cyber-physical systems," *Zidonghua XuebaoActa Autom. Sin.*, vol. 45, pp. 5–24, 2019.

[5] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[6] Yao Liu, Peng Ning, and Michael K. Reiter. "False data injection attacks against state estimation in electric power grids," ACM conference on Computer and communications security (CCS '09), New York, NY, USA, 2009, pp. 21–32.

[7] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 1–33, May 2011.

[8] Md. A. Rahman and H. Mohsenian-Rad, "False data injection attacks with incomplete information against smart power grids," in *2012 IEEE Global Communications Conference*, 2012, pp. 3153–3158.

[9] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Trans. Smart Grid*, vol. 5, no. 4, pp. 1665–1676, Jul. 2014.

[10] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information," *IEEE Trans. Smart Grid*, vol. 8, no. 5, pp. 2239–2248, Sep. 2017.

[11] X. Liu and Z. Li, "Local topology attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[12] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using pca approximation method in smart grid," *IEEE Trans. Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

[13] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 382–390, Jun. 2011.

[14] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

[15] B.-S. Fang, C.-C. Lai, Y.-W. Lu, K.-T. Chen, M. Tasi, and D.-S. Jiang, "A methodology to correct in-fixture measurement of impedance by a machine learning model," in *2019 IEEE 69th Electronic Components and Technology Conference (ECTC)*, 2019, pp. 1704–1709.

[16] T. Sekine, "An estimation method for the capacitance matrix of bundle of wires based on machine learning," in *2018 International Symposium on Electromagnetic Compatibility (EMC EUROPE)*, 2018, pp. 1004–1007.

[17] S. V. Unde and S. S. Dambhare, "Double circuit transmission line parameter estimation using PMU," in *2016 IEEE 6th International Conference on Power Systems (ICPS)*, 2016, pp. 1–4.

[18] D. Liang, H. Guo, and T. Zheng, "Real-time impedance estimation for power line communication," *IEEE Access*, vol. 7, pp. 88107–88115, 2019.

[19] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MAtpower: steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[20] P. L. Donti, Y. Liu, A. J. Schmitt, A. Bernstein, R. Yang, and Y. Zhang, "Matrix completion for low-observability voltage estimation," *ArXiv180109799 Math*, Apr. 2019.

[21] B. Liu, H. Wu, Y. Zhang, R. Yang, and A. Bernstein, "Robust matrix completion state estimation in distribution systems," *2019 IEEE PES General Meeting*, Atlanta, Georgia, GA, 2019.